

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

JACQ NIENABER, on behalf of herself
and all others similarly situated,

Plaintiff,

v.

OVERLAKE HOSPITAL MEDICAL
CENTER,

Defendant.

CASE NO. 2:23-cv-01159-TL

ORDER ON MOTION TO DISMISS

This matter is before the Court on Defendant Overlake Hospital Medical Center's Motion to Dismiss under Rule 12(b)(6). Dkt. No. 17. Having considered Plaintiff's opposition (Dkt. No. 21) and Defendant's reply (Dkt. No. 22), and finding oral argument unnecessary, the Court GRANTS the motion with leave for Plaintiff to amend her complaint.

I. BACKGROUND

The facts alleged in Plaintiff's Class Action Complaint ("Complaint"), which the Court takes as true for the purposes of this Order, are as follows: Plaintiff Jacq Nienaber is a citizen of Washington State and a current patient of Defendant Overlake Hospital Medical Center

1 (“Overlake”). Dkt. No. 1 ¶¶ 35–36. Overlake is a nonprofit healthcare organization
2 headquartered in Bellevue, Washington. *Id.* ¶ 43.

3 Defendant owns and controls two separate websites used by Plaintiff: (1) a public
4 website, www.overlakehospital.org (Defendant’s “Public Website”), through which patients can
5 access information about various conditions and treatments, Overlake’s locations and
6 practitioners, and other general information about Overlake; and (2) the MyChart Patient Portal,
7 <https://mychart.overlakehospital.org/MyChart/Authentication/Login> (Defendant’s “Private
8 Patient Portal” or “MyChart”), where, among other features, patients can input their real time
9 symptoms and experiences and receive feedback based on the medical information they supply.
10 Dkt. No. 1 ¶ 2. As is evident from the link to the website, a patient must log in to use
11 Defendant’s MyChart, which requires a username and password for access. *Id.* ¶ 2 n.1. Plaintiff
12 refers to both Defendant’s Public Website and Private Patient Portal collectively as “the
13 ‘Website’” throughout the Complaint. *Id.* ¶ 2.

14 Through Defendant’s Public Website, patients can access “information about various
15 conditions and treatments, Overlake’s numerous locations and the practitioners at each location,
16 and other general information about Overlake and the services it offers to its patients.” *Id.* ¶ 2.
17 Once logged into MyChart, patients can “input their real time symptoms and experiences on the
18 Website and receive feedback based on the medical information they supply.”¹ *Id.* Plaintiff
19 alleges that she used Defendant’s Website “numerous times” since 2019 to “request and schedule
20 appointments, communicate with healthcare professionals, complete medical forms, and request
21 and review healthcare and billing records.” *Id.* ¶¶ 36–37.

22
23
24 ¹ While the Complaint generally refers to the Website, Plaintiff specifically footnotes Defendant’s Private Patient Portal for these particular functions. Dkt. No. 1 ¶ 2 n.1.

1 Plaintiff alleges that Defendant installed and implemented browser plugins—including
2 the Facebook Tracking Pixel (“Pixel”) and Conversions Application Programming Interface
3 (“Conversions API”), as well as the Google Tag Manager tool—on “its Website,” which
4 “secretly enabled” the unauthorized transmission and disclosure of information.² *Id.* ¶¶ 3–5, 99.

5 The Pixel tracks the people visiting a website and the types of actions that they take,
6 including “how long a person spends on a particular web page, which buttons the person clicks,
7 which pages they view, [and] the text or phrases they type into various portions of the website
8 (such as a general search bar, chat feature, or text box).” *Id.* ¶ 9. “These intercepted
9 communications, intended solely for Defendant, are then transmitted to third parties, including
10 Facebook and Google.” *Id.* ¶ 68. The Conversions API also tracks a website user’s “website
11 interaction, including Private Information, and then transmits this data to Facebook.” *Id.* ¶ 19.
12 The data transmitted includes Plaintiff’s and Class Members’ “health conditions; [] desired
13 medical treatment or therapies; and [] phrases and search queries (such as searches for
14 symptoms, treatment options, or types of providers.” *Id.* ¶ 86. Further, the Pixel additionally
15 transmits website users’ Facebook ID, “thereby allowing individual patients’ communications
16 with Defendant, and the Private Information contained in those communications, to be linked to
17 their unique Facebook accounts and therefore their identity.” *Id.* ¶ 87. The Google Tag Manager
18 tool transmits search phrases typed into the general search bar located on Defendant’s home page
19 to Google. *Id.* ¶¶ 99–100.

20 Plaintiff reasonably expected that her online communications with Defendant were solely
21 between herself and Defendant, expected Defendant would safeguard her private information
22 based on Defendant’s privacy policies, and did not consent to the use of her private information

23
24 ² Plaintiff asserts, and the Court acknowledges, that “there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like the Conversions API without access to the host server.” *Id.* ¶ 71.

1 by third parties. *Id.* ¶¶ 38–39. Plaintiff is a Facebook user and alleges that “shortly after using
2 Defendant’s Website, Plaintiff has seen numerous targeted advertisements on Facebook related
3 to her medical conditions and treatments sought through Overlake.” *Id.* ¶¶ 41–42.

4 Plaintiff contends that Defendant’s transmissions of information via the Pixel,
5 Conversions API, and Google Tag Manager are in violation of its own privacy policies, HIPAA
6 standards, and industry standards. *Id.* ¶¶ 104–08 (privacy policies), 109–15 (HIPAA standards),
7 116–20 (industry standards). Defendant’s privacy policies state that “[a]ny information
8 submitted by users of the Sites is for the exclusive use of Overlake Medical Center and Clinics as
9 well as our contractors that are involved in the operation of Overlake Medical Center and
10 Clinics’ activities and website operations” *Id.* ¶ 106. And the policies purport to enumerate the
11 ways in which Defendant will use and disclose patients’ medical information, none of which,
12 Plaintiff says, cover disclosure to third parties for marketing purposes. *Id.* ¶ 107. Plaintiff also
13 looks to guidance from the Department of Health and Human Services, which indicates that
14 patient status and other identifying information are protected information under HIPAA. *Id.* ¶¶
15 110–13. Finally, Plaintiff points to various AMA Code of Medical Ethics Opinions concerning
16 the privacy of patient data and communications that she alleges Defendant failed to abide by as
17 evidence that Defendant violated industry standards. *Id.* ¶¶ 118–20.

18 II. LEGAL STANDARD

19 A defendant may seek dismissal when a plaintiff fails to state a claim upon which relief
20 can be granted. Fed. R. Civ. P. 12(b)(6). In reviewing a FRCP 12(b)(6) motion to dismiss, the
21 Court takes all well-pleaded factual allegations as true and considers whether the complaint
22 “state[s] a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678
23 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). While “[t]hreadbare
24 recitals of the elements of a cause of action, supported by mere conclusory statements” are

insufficient, a claim has “facial plausibility” when the party seeking relief “pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 672. “When reviewing a dismissal pursuant to Rule . . . 12(b)(6), ‘we accept as true all facts alleged in the complaint and construe them in the light most favorable to plaintiff[], the non-moving party.’” *DaVinci Aircraft, Inc. v. United States*, 926 F.3d 1117, 1122 (9th Cir. 2019) (alteration in original) (quoting *Snyder & Assocs. Acquisitions LLC v. United States*, 859 F.3d 1152, 1156–57 (9th Cir. 2017)).

“If a complaint is dismissed for failure to state a claim, leave to amend should be granted unless the court determines that the allegation of other facts consistent with the challenged pleading could not possibly cure the deficiency.” *Or. Clinic, PC v. Fireman’s Fund Ins. Co.*, 75 F.4th 1064, 1073 (9th Cir. 2023) (citing *Schreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806 F.2d 1393, 1401 (9th Cir. 1986)). A revised complaint would replace the current complaint. *Lacey v. Maricopa Cty.*, 693 F.3d 896, 925 (9th Cir. 2012) (en banc) (“the general rule is that an amended complaint supersedes the original complaint and renders it without legal effect”).

III. DISCUSSION

A. Plaintiff Does Not Allege the Disclosure of Personally Identifiable Information or Protected Health Information

In this case, Plaintiff alleges that Defendant misuses Plaintiff’s and other website users’ confidential personally identifiable information (“PII”) and protected health information (“PHI”) (collectively referred to as “Private Information”). Dkt. No. 1 ¶ 1. The principal theory of Plaintiff’s case, underlying all claims, is that Defendant transmits the Private Information that patients input into Defendant’s websites to third parties without patients’ consent. However, throughout the complaint, Plaintiff refers to Defendant’s Public Website and Private Patient Portal collectively as “the Website.” Dkt. No. 1 ¶ 2.

1 As other courts within this Circuit have acknowledged, the transmission of information
2 submitted to a *private patient portal*—such as a user clicking on the “log in” button on that
3 webpage—reveals patient status, which in and of itself is protected health information. *See, e.g.,*
4 *In re Meta Pixel Healthcare Litigation (In re Meta Pixel I)*, 647 F. Supp. 3d 778, 791–93 (N.D.
5 Cal. 2022); *Cousin v. Sharp Healthcare (Cousin I)*, 681 F. Supp. 3d 1117, 1123–24 (S.D. Cal.
6 July 12, 2023). The collection and transmission of information from *unauthenticated* web pages
7 (*i.e.*, pages that do not require a user to log in to access the website) may be actionable as well if
8 the information disclosed demonstrates that the plaintiff’s interactions plausibly relate to the
9 provision of healthcare, or if the information connects a particular user to a particular healthcare
10 provider (*i.e.*, patient status). *See Cousin v. Sharp Healthcare (Cousin II)*, No. C22-2040, 2023
11 WL 8007350, *2–3 (S.D. Cal. Nov. 17, 2023); *In re Meta Pixel I*, 647 F. Supp. 3d at 793; *In re*
12 *Meta Healthcare Pixel Litigation (In re Meta Pixel II)*, No. C22-3580, 2024 WL 333883, *2–3
13 (N.D. Cal. Jan. 29, 2024). However, where nothing but browsing activity on a publicly available
14 website is transmitted, courts within this circuit have held that “the URLs, or the content of the
15 pages located at those URLs, [do not relate] ‘to the past, present, or future physical or mental
16 health or condition of an individual.’” *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955 (N.D.
17 Cal. 2017) (quoting 45 C.F.R. § 160.103), *aff’d* 745 F. App’x 8 (9th Cir. 2018); *see also Cousin*
18 *I*, 681 F. Supp. 3d at 1123.

19 Defendant argues that Plaintiff only makes allegations about “public website browsing,”
20 and that Plaintiff cannot maintain her claims to the extent that they are based upon the theory that
21 Defendant’s sharing of Plaintiff’s browsing activity constitutes sharing of Private Information.
22 Dkt. No. 17 at 13. Thus, whether the allegations concern Defendant’s Public Website or Private
23 Patient Portal may make a significant difference.

1 **1. Defendant’s Private Patient Portal**

2 There are only two sentences in Plaintiff’s Complaint that describe her actual engagement
 3 with Defendant’s websites: (1) “Plaintiff used [Defendant’s] Website to find and obtain medical
 4 treatment,” Dkt. No. 1 ¶ 35; and (2) “Plaintiff [] used Defendant’s Website to conduct the
 5 following activities: request and schedule appointments, communicate with healthcare
 6 professionals, complete medical forms, and request and review healthcare and billing records.”
 7 *Id.* ¶ 37. Except for requesting and scheduling appointments, it appears the other actions can only
 8 be done while logged in to Defendant’s MyChart. While it is not necessary for Plaintiff to
 9 provide specific medical details, she must allege more than she has.

10 In *Doe v. Regents of Univ. of California*, 672 F. Supp. 3d 813 (N.D. Cal. 2023), upon
 11 which Plaintiff relies, the court found that plaintiff’s allegations survived a motion to dismiss
 12 where:

13 [Plaintiff] entered medical information, including information
 14 relating to her heart issues and high blood pressure, into the patient
 15 portal . . . that UC Regents intentionally incorporated Meta Pixel
 16 on the UCSF website and password protected MyChart portal,
 17 disclosing and allowing Meta to intercept her and class members’
 18 data . . . that *after she entered her information into UCSF’s*
 19 *patient portal*, she began receiving advertisements on Facebook for
 20 high blood pressure medication as well as targeted email
 21 advertisements relating to the same . . . [and] that she used the
 22 same email address to register for both her MyChart and her
 23 Facebook account, [providing] a plausible means by which her
 24 information could be matched to her Facebook profile.

Id. at 819 (emphasis added). Here, Plaintiff vaguely states that she “communicate[d] with
 healthcare professionals” and “complete[d] medical forms.” Dkt. No. 1 ¶ 37. However, Plaintiff
 makes no allegations as to the type of information she provided to Defendant through MyChart
 or that Defendant transmitted Private Information *of hers* to third parties through the Private
 Patient Portal. *See* Dkt. No. 1 ¶¶ 36–42. Indeed, Plaintiff does not even clearly allege whether

1 she used MyChart or the Public Website to request or schedule appointments. *See id.* Instead, the
2 Complaint discusses a hypothetical example of a patient scheduling an appointment where the
3 user is then directed to communicate information including the type of medicine being sought
4 and the type of appointment being scheduled. *Id.* ¶ 90. But Plaintiff neither alleges that *she* tried
5 to schedule an appointment through MyChart nor that *she* entered the type of medicine she
6 sought or the type of appointment being scheduled (which would undoubtedly be protected
7 health information), or that the Pixel transmitted *her* information to Facebook. *See id.* ¶¶ 90–98.
8 All of these types of information are easily and clearly within Plaintiff’s control, and Plaintiff
9 cannot maintain her theory of the case as to the MyChart website absent concrete factual
10 allegations that her Private Information entered on Defendant’s Private Patient Portal was
11 disclosed.

12 Further, in giving an example of using the website to schedule an appointment, Plaintiff
13 includes one image from a generic MyChart page. *Id.* ¶ 90. Plaintiff clearly tries to suggest she
14 browsed Defendant’s Private Patient Portal and that Private Information from it was transmitted
15 to third parties. But the examples given to try to establish disclosure only relate to Defendant’s
16 Public Website, where a patient may also schedule an appointment. *Id.* ¶¶ 75, 94, and 97. All
17 three of the examples are clearly tied to www.overlakehospital.org, and the examples given of
18 the information sent to Facebook are from the Public Website appointments page, not the
19 MyChart page. *Id.* ¶¶ 94, 97. Plaintiff claims that “this particular webpage”—referring to the
20 MyChart image in Paragraph 90—contains Defendant’s Pixel. *Id.* ¶ 93. However, the very next
21 paragraph that is supposed to show Defendant’s Pixel on the webpage is from Defendant’s
22 Public Website.³ *Id.* ¶ 94.

23
24 ³ Given the examples Plaintiff provides with her Complaint, it appears she could also provide the same information
with regard to Defendant’s Private Patient Portal.

1 Plaintiff's response brief only addresses whether disclosures made from browsing a
2 public website may be actionable and not whether they allege any information was disclosed
3 from the Private Patient Portal. Dkt. No. 21 at 11–12. The skeletal information in the Complaint
4 leads the Court to agree with Defendant that Plaintiff only makes allegations regarding Private
5 Information being disclosed from Defendant's Public Website.

6 **2. Defendant's Public Website**

7 Disclosure through publicly available webpages that, plausibly relate to the provision of
8 healthcare or connect a particular user to a particular healthcare provider may be actionable.
9 *Cousin II*, 2023 WL 8007350, at *2–3; *In re Meta Pixel I*, 647 F. Supp. 3d at 793; *In re Meta*
10 *Pixel II*, 2024 WL 333883, at *2–3. However, in the case at hand, Plaintiff does not make
11 sufficient factual allegations to demonstrate that any such information was transmitted to third
12 parties by Defendant through its Public Website. Plaintiff alleges that she used Defendant's
13 website to request and schedule appointments. Dkt. No. 1 ¶ 37. But Plaintiff provides no
14 additional factual information tying her actual activities to the allegations made by the
15 hypothetical purportedly demonstrating disclosure of Private Information. For example, Plaintiff
16 provides no information as to whether she used Defendant's Public Website to schedule an
17 appointment or regarding what information she entered on Defendant's Public Website
18 containing information-sharing browser plugins. *See generally* Dkt. No. 1 ¶¶ 37, 75, 90–98.

19 Further, the disclosure of browsing activity on a publicly available website that does not
20 relate “to the past, present, or future physical or mental health or condition of an individual” is
21 not actionable. *See Smith*, 262 F. Supp. 3d at 954–55 (quoting 45 C.F.R. § 160.103). The
22 example given in the Complaint only shows that the fact that a user viewed the “Schedule an
23 Appointment” page on Defendant's Public Website was disclosed to a third party. Dkt. No. 1
24 ¶¶ 94, 96. Plaintiff also alleges that when a patient uses the general search bar located on

1 Defendant's website homepage, the exact text and phrases typed by the user are transmitted to
2 Google via the Google Tag Manager. *Id.* ¶¶ 99–102. But the example given simply shows a
3 search on Defendant's Public Website for the word "cancer" which pulled up generic
4 information regarding certain services and general information on prostate cancer. *Id.* ¶¶ 99–101.
5 Plaintiff does not allege that the text and phrases are transmitted in addition to any information
6 identifying the user as a patient, nor does she make specific allegations as to her use of this
7 general search bar. *See id.* ¶¶ 37, 99–102. Plaintiff contends that *Doe v. Bon Secours Mercy*
8 *Health*, No. C20-2633, 2021 WL 9939010 (Ohio C.P. Nov. 22, 2021) supports her contention
9 that allegations of public browsing activity are actionable. *See* Dkt. No. 21 at 11. But in *Bon*
10 *Secours*, the plaintiff had made allegations that "the information disclosed to third parties
11 includes the fact that a visitor to defendant's [public] website is a patient of defendant." *Bon*
12 *Secours*, 2021 WL 9939010, at *2. Plaintiff here makes no such allegations.

13 In any event, courts have dismissed similar allegations regarding hypothetical examples
14 of data sharing. The Central District of California recently dismissed comparable privacy claims
15 where:

16 Plaintiffs fail to allege what, if any, medical information or
17 medical records were transmitted or disclosed. Notably, Plaintiffs'
18 Complaint is 90 pages long but includes less than four pages of
19 vague allegations about Plaintiffs and their experiences with
20 Defendant. The Complaint is replete with conjectures and
21 hypothetical scenarios and patients. Plaintiffs fail to allege any
22 specificity as to what medical information was allegedly disclosed
23 or when it was disclosed. B.K. states she started using the Website
24 over three years ago and started receiving unsolicited ads "shortly
after" but provides no more information about the alleged
disclosures. N.Z. alleges the same pattern but states that it occurred
"over seven years ago."

1 *B.K. v. Eisenhower Medical Center*, No. C23-2092, 2024 WL 878100, at *4 (C.D. Cal. Fed. 29,
2 2024) (internal citations omitted). The Northern District of Illinois ruled similarly in another
3 healthcare provider data-sharing case, holding:

4 Kurowski's allegations are far too vague to allow an inference to be
5 drawn that Rush was actually disclosing IHI as it is
6 unambiguously defined by HIPAA, rather than just metadata.
7 Kurowski contends that it would be unreasonable to expect her to
8 disclose that type of intimate information in her complaint. But
9 that contention lacks merit. Kurowski could have requested to file
10 the complaint under seal. Moreover, Kurowski cannot reasonably
11 expect to bring a lawsuit related to the invasion of her medical
12 privacy and completely evade revealing what it is that she alleges
13 Rush disclosed to third parties.

14 *Kurowski v. Rush System for Health (Kurowski II)*, 683 F. Supp. 3d 836, 843 (N.D. Ill. 2023);
15 *see also Kurowski v. Rush System for Health (Kurowski III)*, No. C22-5380, 2023 WL 8544084,
16 at *3 (N.D. Ill. Dec. 11, 2023) (holding that claims survived after complaint was amended to
17 include “additional factual allegations regarding the information [plaintiff] contends was
18 transmitted to third parties with Rush’s knowledge”). Here, Plaintiff’s two sentences of specific
19 allegations coupled with the hypotheticals offered is simply not enough.

20 That is not to say that interactions on publicly available websites cannot constitute PHI.
21 To the contrary, in *Cousin*, following the court’s dismissal, plaintiffs amended their complaint to
22 include further allegations about their interactions on defendant’s website. *Cousin II*, 2023 WL
23 8007350, at *1. The court found that:

24 Plaintiff Cousin alleges that she used Sharp’s website to search for
a primary care physician. Namely, she filtered the results of
Sharp's physician directory by, among other things, specialty. This
just narrowly survives dismissal by demonstrating that her
interactions plausibly relate to the provision of health care.
Plaintiffs Camus and Barbat, on the other hand, set forth their
particular medical conditions and allege that they searched
Defendant's website for doctors who specialize in these conditions
and for information about their conditions (i.e., symptoms,
treatments, procedures). Camus also alleges she booked an

1 appointment to obtain treatment for a medical condition. These
2 interactions plausibly convey information about a present medical
condition and the provision of medical care covered by HIPAA.

3 *Id.* at *3 (internal citations omitted); *see also Toy v. Life Line Screening of Am. LTD*, No. C23-
4 4651, 2024 WL 1701263, at *1 (N.D. Cal. Mar. 19, 2024) (“Toy sufficiently alleges a concrete
5 harm. The complaint alleges that Toy used Life Line’s website to order at-home health tests and
6 view her results, and that the URL of the webpage, which contains information about what tests
7 she purchased, were shared without her permission with Facebook via the Facebook Pixel, an
8 invisible tracker that Life Line had embedded in its website.”). But Plaintiff has made no
9 allegations of her interactions with Defendant’s websites, let alone any allegations showing that
10 her interactions plausibly related to the provision of healthcare or were shared by Defendant. In
11 fact, Plaintiff’s allegations as to herself are disconnected from any allegations of information
12 sharing by Defendant. *See, e.g.*, Dkt. No. 1 ¶ 37. Her claims cannot survive absent this factual
13 support.

14 With this in mind, the Court turns to each of Plaintiff’s class-wide claims.

15 **B. Count I: Negligence**

16 Plaintiff brings a claim for negligence on behalf of herself and of the putative national
17 class. Dkt. No. 1 ¶¶ 154–65. Defendant contends that Plaintiff has failed to establish duty,
18 breach, and cognizable damages, and that the negligence claims is otherwise barred by the
19 economic loss rule. Dkt. No. 17 at 13–14.

20 Under Washington law, negligence requires “(1) the existence of a duty to the plaintiff,
21 (2) a breach of that duty, (3) a resulting injury, and (4) the breach as the proximate cause of that
22 injury.” *Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1156 (W.D. Wash.
23 2017) (citing *Degal v. Majestic Mobile Manor*, 129 Wn.2d 43, 914 P.2d 728, 731 (1996)). “The
24 existence of a duty ‘is a question of law and depends on mixed considerations of logic, common

1 sense, justice, policy, and precedent.” *Id.* (quoting *Snyder v. Med. Serv. Corp.*, 145 Wn.2d 233,
2 35 P.3d 1158, 1164 (2001)). Duty may be predicated “on violation of statute or of common law
3 principles of negligence.” *Id.* (quoting *Jackson v. City of Seattle*, 158 Wn. App. 647, 244 P.3d
4 425, 428 (2010)). Plaintiff alleges that Defendant owed a duty of care to Plaintiff and the
5 putative national class to keep their PHI confidential because Defendant is a health care provider
6 under the Health Care Information Act (“HCIA”), and because Defendant’s own privacy policy
7 establishes that it owes a duty to Plaintiff. Dkt. No. 21 at 12–14. Defendant primarily relies upon
8 its argument that Plaintiff’s allegations are limited to public browsing activity, arguing that there
9 is no duty to protect such activity. Dkt. No. 22 at 7.

10 Plaintiff first argues that “as a health care provider, Defendant owes a duty to keep health
11 care information confidential under the Health Care Information Act (“HCIA”).” Dkt. No. 21
12 at 12. To determine whether a duty of care exists based upon a statutory violation, Washington
13 courts have adopted the Restatement test, which “requires that the injured person be within the
14 class of persons the statute was enacted to protect,” the particular interest of the plaintiff be
15 within the scope of the interest protected by the statute, the harm be the kind the statute was
16 enacted to protect, and the hazard causing the harm be the type the statute was enacted to protect.
17 *Schooley v. Pinch’s Deli Market, Inc.*, 134 Wn.2d 468, 474–75, 951 P.2d 749 (1998) (citing
18 *Hansen v. Friend*, 118 Wn.2d 476, 480, 824 P.2d 483 (1992)); Rest. 2d Torts § 286. The
19 legislative findings accompanying the HCIA state that “[i]n order to retain the full trust and
20 confidence of patients, health care providers have an interest in assuring that health care
21 information is not improperly disclosed and in having clear and certain rules for the disclosure of
22 health care information.” RCW 70.02.005. “Health care information” as defined under the
23 HCIA, is “any information . . . that identifies or can readily be associated with the identity of a
24 patient and directly relates to the patient’s health care.” RCW 70.02.20. Plaintiff here is a patient

1 of Defendant (Dkt. No. 1 ¶ 36) and is thus within the class of persons that the HCIA was enacted
 2 to protect. Further, the willful disclosure of health care information is the type of harm the HCIA
 3 was enacted to protect. *See Seattle Children's Hospital v. King County*, 16 Wn. App. 2d 365, 483
 4 P.3d 785, 794 (2020) ("The HCIA recognizes that '[h]ealth care information is personal and
 5 sensitive information that if improperly used or released may do significant harm to a patient's
 6 interests in privacy, health care, or other interests.'" (quoting RCW 70.02.005(1)) (alteration in
 7 original)). Plaintiff has therefore alleged a duty under the HCIA.

8 Plaintiff also argues that Defendant's own privacy policy establishes a duty to Plaintiff.
 9 *See, e.g.*, Dkt. No. 21 at 13–14; Dkt. No. 1 ¶¶ 106–08. Defendant's online privacy notice states:

10 [a]ny information submitted by users of the Sites is for the
 11 exclusive use of Overlake Medical Center and Clinics as well as
 12 our contractors that are involved in the operation of Overlake
 13 Medical Center and Clinics' activities and website operation
 We will not share your information with any third party outside of
 our organization unless the third party provides services on our
 behalf . . . or if it is required by law."

14 Dkt. No. 1 ¶ 106. Defendant does not appear to dispute that its privacy policy establishes a duty
 15 to safeguard PHI but argues that the Complaint only alleges the disclosure of public website
 16 browsing data. Dkt. No. 22 at 7.

17 Finally, Plaintiff argues that Defendant's alleged misfeasance creates a duty to Plaintiff.
 18 *See* Dkt. No. 21 at 13–14. "Washington courts have held that 'a duty to guard against a third
 19 party's foreseeable criminal conduct exists where an actor's own affirmative act has created or
 20 exposed another to a recognizable high degree of risk of harm through such misconduct, which a
 21 reasonable person would have taken into account.'" *Buckley v. Santander Consumer USA, Inc.*,
 22 No. C17-5813, 2018 WL 1532671, at *5 (W.D. Wash. Mar. 29, 2018) (quoting *Parilla v. King*
 23 *County*, 138 Wn. App. 427, 439, 157 P.3d 879 (2007)). "Under such a theory, it is necessary that
 24 the defendant have engaged in some 'misfeasance,' which 'necessarily entails the creation of a

1 new risk of harm to the plaintiff.” *Id.* (quoting *Robb v. City of Seattle*, 176 Wn.2d 427, 437, 295
2 P.3d 212 (2013)). The intentional disclosure of personal information by Defendant to an
3 unauthorized third party, as Plaintiff has alleged, constitutes an affirmative act, or misfeasance.
4 *See id.* “It is foreseeable that providing a customer's private information . . . creates a new risk of
5 harm to the customer, particularly of identity theft or other fraudulent schemes based on the
6 exploitation of such data.” *Id.* Plaintiff has thus alleged a duty under the misfeasance theory.

7 While Plaintiff establishes the existence of a duty, satisfying the first prong of the
8 negligence analysis, Plaintiff fails to allege facts sufficient to establish a breach of that duty. As
9 detailed above, Plaintiff has not made specific allegations as to what information she gave to
10 Defendant, and what information Defendant in turn shared with third parties, nor has she alleged
11 that Defendant shared information that can be used to readily identify her. *See* Dkt. No. 1 ¶¶ 7,
12 35–42, 50–103, 123–31, 246. While Plaintiff has made hypothetical allegations of information-
13 sharing, Plaintiff must plead facts showing (or supporting the inference) that *her* PHI was shared
14 with Defendant and by Defendant to third parties. Plaintiff has therefore not alleged a breach of
15 Defendant’s duty to safeguard PHI under the HCIA, its privacy policy, or the misfeasance
16 theories of duty. For this reason, Plaintiff’s negligence claim fails.

17 As it seems likely plaintiff will be able to properly amend her complaint, the Court finds
18 it worthwhile to address the Parties’ arguments regarding damages. Plaintiff argues that she
19 adequately alleges damages in the form of the diminished value of her sensitive health and
20 personal information.⁴ Dkt. No. 21 at 14–15. Defendant contends that Plaintiff must “plead facts
21 showing that she lost the opportunity to sell her information or that the value of [her] information
22 was somehow diminished after it was collected by Facebook,” or “recover on an overpayment
23

24 ⁴ Plaintiff’s Complaint only asserts that “Plaintiff and Class Members are entitled to nominal, punitive,
compensatory and/or consequential damages suffered as a result of the Data Breach.” Dkt. No. 1 ¶ 164.

theory.” Dkt. No. 17 at 14. Plaintiff is correct that damages are adequately alleged where a plaintiff alleges “a heightened risk of future identity theft, loss of privacy with respect to highly sensitive information, loss of time, and risk of embarrassment,” rather than pure economic damages. *Flores-Mendez v. Zoosk, Inc.*, No. C20-4929, 2021 WL 308543, at *3–4 (N.D. Cal. Jan. 30, 2021). However, Plaintiff has alleged no such facts in her Complaint and, therefore, has not alleged any damages.

For the foregoing reasons, Plaintiff’s negligence claim is DISMISSED with leave to amend.

C. Count II: Invasion of Privacy

Plaintiff brings a claim for invasion of privacy on behalf of herself and the putative national class. Dkt. No. 1 ¶¶ 166–79. “Washington common law recognizes a ‘protectable interest in privacy [that] is generally held to involve four distinct types of invasion: intrusion, disclosure, false light and appropriation.’” *Buckley v. Santander Consumer USA, Inc.*, No. C17-5813, 2018 WL 1532671 (W.D. Wash. Mar. 29, 2018) (quoting *Eastwood v. Cascade Broad. Co.*, 106 Wn.2d 466, 469, 722 P.2d 1295 (1986)); *see also Armijo v. Yakima*, No. C11-3114, 2012 WL 2576624, *2 (E.D. Wash. July 3, 2012). Plaintiff argues that she prevails under both an intrusion upon seclusion and a public disclosure of private facts theory of her claim. Dkt. No. 21 at 15.

1. Intrusion Upon Seclusion

“To prevail on an intrusion on seclusion claim, a plaintiff must prove that the defendant (1) deliberately intruded; (2) into the plaintiff’s solitude, seclusion, or private affairs; (3) in a manner that would be highly offensive to a reasonable person.” *Armijo*, 2012 WL 2576624, at *2 (citing *Fisher v. State ex rel. Dep’t of Health*, 125 Wn. App. 869, 106 P.3d 836 (2005)). “Invasion of privacy by intrusion consists of a deliberate intrusion, physical or otherwise, into a person’s solitude, seclusion, or private affairs.” *Fisher*, 106 P.3d at 840; *see also Poore-Rando v.*

1 *United States*, No. C16-5094, 2017 WL 5756871, at *2 (W.D. Wash. Nov. 28, 2017) (“[A]n actor
2 commits an intentional intrusion only if he believes, or is substantially certain, that he lacks the
3 necessary legal or personal permission to commit the intrusive act.”) (quoting *O’Donnell v.*
4 *United States*, 891 F.2d 1079, 1083 (3d Cir. 1989) (alteration in original)).

5 Plaintiff contends that “Defendant intruded upon her seclusion by deliberately planting a
6 bug on her web browser that surreptitiously forced her to duplicate her communications with
7 Defendant and disclose them to Facebook, Google, and other third parties.” Dkt. No. 21 at 15–
8 16. Defendant primarily relies on *Kurowski v. Rush System for Health (Kurowski I)*, 659 F. Supp.
9 3d 931 (N.D. Ill. 2023), to argue that “the alleged intrusion, if any, was carried out by a third
10 party” and is therefore not actionable against Defendant. Dkt. No. 17 at 15.⁵

11 *Kurowski I* addressed an invasion of privacy claim under Illinois common law where the
12 plaintiff alleged “that Rush [(a university hospital system)] intruded by deploying third-party
13 source code that caused personally identifiable patient data to be disclosed to third parties.” 659
14 F. Supp. 3d at 943. Like Washington, Illinois recognizes a common law action for invasion of
15 privacy by intrusion upon seclusion, and similarly describes the “core of [the] tort” as “the
16 offensive prying into the privacy domain of another.” *Id.*; see also *Fisher*, 106 P.3d at 840
17 (“Invasion of privacy by intrusion *consists of a deliberate intrusion*, physical or otherwise, into a
18 person's solitude, seclusion, or private affairs.” (emphasis added)). The *Kurowski I* court
19 determined that “the core of [plaintiff’s] claim is Rush’s deployment of third-party source code
20 that causes the transmission of patient data”— “[i]n other words, the harm for which Rush is
21 responsible, if any, is its disclosure of patient data[. . .], not the obtaining of that data.” 659 F.
22 Supp. 3d at 943–44. The Court finds this reasoning persuasive. Plaintiff’s claim for invasion of
23

24 ⁵ Plaintiff contends that *Kurowski I*’s holding is “contrary to caselaw from within the Ninth Circuit.” Dkt. No. 21 at 17. But Plaintiff cites to no caselaw supporting this proposition. *Id.*

1 privacy is rooted in her allegations that she willfully shared private information with Defendant,
2 which Defendant then shared with third parties. *See generally* Dkt. No. 1. Because Plaintiff
3 voluntarily shared her information with Defendant, there was no *intrusion* upon Plaintiff's
4 solitude, seclusion, or private affairs by Defendant. *See Buckley*, 2018 WL 1532671, at *7
5 ("Because Santander allegedly financed Buckley's vehicle purchase, Santander possessed the
6 necessary legal permission to acquire Buckley's personal information. To the extent that Buckley
7 complains that Santander deliberately passed this information along to an unauthorized third
8 party, that is not a claim for intrusion but rather disclosure."). Contrary to Plaintiff's argument,
9 this does not serve to imply that "the postal service could let strangers on the street open
10 someone's outgoing mail" (Dkt. No. 21 at 17), it only means that such an act would not be
11 actionable as an invasion of privacy claim under the specific theory of intrusion upon seclusion.

12 **2. Public Disclosure of Private Facts**

13 "To prevail on a public disclosure of private facts claim, a plaintiff must prove that the
14 defendant (1) intentionally disclosed private facts; (2) that were not of legitimate concern to the
15 public; (3) which disclosure would be highly offensive to a reasonable person." *Armijo*, 2012
16 WL 2576624, at *2 (citing *Adams v. King County*, 164 Wn.2d 640, 192 P.2d 891 (2008)). "This
17 cause of action is distinguished from the tort of intrusion upon seclusion in that 'publicity is an
18 essential element [of] an action based upon the defendant's public disclosure of private facts.'" *Id.*
19 (quoting David K. DeWolf & Keller W. Allen, 16A *Washington Practice Series* § 20.5 (3d
20 ed.)) (alteration in original). "Publicity . . . means communication to the public at large so that
21 the matter is substantially certain to become public knowledge . . . ; communication to a single
22 person or a small group does not qualify." *Fisher*, 106 P.3d at 840–41.

23 Plaintiff argues that she succeeds on the "publication" theory of invasion of privacy
24 because Defendant "has taken information that is private and shown it to some of the world's

1 largest advertising companies, who use it for targeted marketing and advertising Plaintiff did not
2 authorize.” Dkt. No. 21 at 17. Defendant contends that Plaintiff’s claim under this theory fails
3 because Plaintiff does not allege that the communication was to the public at large. Dkt. No. 22
4 at 9. Defendant further argues that Plaintiff has failed to allege any conduct that is “highly
5 offensive” to a person with ordinary sensibilities. Dkt. No. 17 at 16.

6 “[P]ublicity for the purposes of [a public disclosure of private facts claim] means
7 communication to the public at large so that the matter is substantially certain to become public
8 knowledge.” *Fisher*, 106 P.2d at 840–41. “[C]ommunication to a single person or a small group
9 does not qualify.” *Id.* at 841. The disclosure of PHI or PII to Facebook and Google, as Plaintiff
10 alleges, does not meet this standard of publicity. *See In re MCG Health Data Security Issue*
11 *Litigation*, No. C22-0849, 2023 WL 3057428, at *6 (W.D. Wash. Mar. 27, 2023) (“Plaintiffs
12 allege that cybercriminals obtained the information. There are no allegations that MCG Health
13 publicized Plaintiffs’ private information to more than a small group of people.”); *Buckley*, 2018
14 WL 1532671, at *7 (holding that pleadings lacked necessary allegations to support publicity
15 element where plaintiff alleged disclosure of personal information to a third party). While
16 Plaintiff makes conclusory allegations that Facebook sells the Private Information it obtains from
17 Defendant to additional third-party marketers (Dkt. No. 1 ¶ 22), she does not offer any factual
18 support for these claims, nor does she identify any specific marketers that she believes are in
19 receipt of her information. Further, Plaintiff does not allege that the information shared by
20 Defendant will become available to the public *at large*; to the contrary, Plaintiff alleges that the
21 information is shared with Facebook and, in turn, is being used by Facebook to target Plaintiff
22 herself. *See* Dkt. No. 1 ¶¶ 30, 31, 42.

23 Even if the alleged disclosure was considered public disclosure, Plaintiff has not
24 adequately identified the personal PHI she alleges was publicized for the Court to determine

whether any such disclosure would be highly offensive to a person with ordinary sensibilities. *See, e.g., Reid v. Pierce County*, 136 Wn.2d 195, 961 P.2d 333 (1998) (holding that disclosure of autopsy records and photographs of a relative would be highly offensive to a person with ordinary sensibilities).

For the foregoing reasons, Plaintiff's invasion of privacy claim is DISMISSED with leave to amend.

D. Count III: Breach of Confidence

Plaintiff brings a claim for breach of confidence on behalf of herself and the putative national class. Dkt. No. 1 at 41–42. Defendant contends that breach of confidence is not recognized as a common law cause of action under Washington law. Dkt. No. 17 at 18.

As Defendant correctly states, Washington has not recognized breach of confidence as a common law cause of action. *Snapp v. Burlington Northern Santa Fe Ry.*, No. C10-5577, 2012 WL 3157137, at *4–5 (W.D. Wash. Aug. 3, 2012) (citing *Hines v. Todd Pacific Shipyards Corp.*, 127 Wn. App. 356, 112 P.3d 522 (2005)), *overturned on other grounds by Snapp v. United Transp. Union*, 547 F. App'x 824 (9th Cir. 2013). While Washington does recognize “a cause of action against a physician for unauthorized disclosure of privileged information” under Chapters 7.70 and 70.02 of the Revised Code of Washington, *Berger v. Sonneland*, 144 Wn.2d 91, 105–07, 26 P.3d 257, 265–66 (2001), those are statutory claims distinct from the common law breach of confidence claim that Plaintiff brings.

For the foregoing reasons, Plaintiff's breach of confidence claim is DISMISSED.

E. Count IV: Breach of Implied Contract

Plaintiff brings a claim for breach of implied contract on behalf of herself and the putative national class. Dkt. No. 1 ¶¶ 188–94. Defendant argues that Plaintiff fails to plead facts

1 showing mutual assent and consideration, and that its privacy policy does not give rise to a
2 breach of contract. Dkt. No. 17 at 10.

3 “To prevail on a breach of implied contract claim, a plaintiff must demonstrate that [an]
4 implied contract exists based on the acts of the parties involved and in light of the surrounding
5 circumstances.” *Leslie v. Fidelity Nat. Title Ins. Co.*, 598 F. Supp. 2d 1176, 1184 (W.D. Wash.
6 2009) (citing *Caughlan v. Int’l Longshoremen’s and Warehousemen’s Union*, 52 Wn.2d 656,
7 328 P.2d 707 (1958)). Washington recognizes two classes of implied contracts: those implied in
8 fact, and those implied in law. *Young v. Young*, 164 Wn.2d 477, 191 P.3d 1258 (2008) (citing
9 *Chandler v. Wash. Toll Bridge Auth.*, 17 Wn.2d 591, 137 P.2d 97 (1943)). Plaintiff alleges a
10 contract implied in fact. Dkt. No. 21 at 18.

11 A contract implied in fact “requires mutual assent of the parties, but a trial court may
12 ‘deduce mutual assent from the circumstances, whereby the court infers a contract based on a
13 course of dealings between the parties or a common understanding within a particular
14 commercial setting.’” *Leslie*, 598 F. Supp. 2d at 1184 (quoting *Hoglund v. Meeks*, 139 Wn. App.
15 854, 870–71, 170 P.3d 37 (2007)). “Whether parties manifested mutual assent to form a contract
16 is generally a factual question.” *Id.* (quoting *Hoglund*, 139 Wn. App. at 871).

17 Plaintiff contends that when she and the other putative class members “provided their
18 user data to Defendant in exchange for services, they entered into an implied contract pursuant to
19 which Defendant agreed to safeguard and not disclose their Private Information without
20 consent.” Dkt. No. 1 ¶ 189. However, these facts are insufficient to allege the existence of an
21 implied contract. As Plaintiff acknowledges, “[t]he services [giving rise to the contract] must be
22 rendered under such circumstances as to indicate that the person rendering them expected to be
23 paid therefor, and that the recipient expected, or should have expected, to pay for them.” *Johnson*
24 *v. Nasi*, 50 Wn.2d 87, 91, 309 P.2d 380 (1957); Dkt. No. 21 at 18. But Plaintiff has made no

1 allegations that she paid Defendant for any medical services, nor has she made any additional
2 allegations regarding any consideration received by Defendant for its promise to safeguard
3 Plaintiff's information. *See* Dkt. No. 1 ¶¶ 35–42, 188–94. Plaintiff therefore fails to allege the
4 existence of a valid contract supported by mutual assent and consideration.

5 In each of the cases that Plaintiff relies on, the court pointed to more substantial
6 allegations that it held supported the existence of an implied contract. For example, in *Doe v.*
7 *Boone Health, Inc.*, the court held the plaintiff had adequately stated a claim for an implied-in-
8 fact contract where:

9 Plaintiff alleges that Defendants manifested an implicit promise to
10 provide medical services, to institute reasonable measures to
11 protect the confidentiality of his medical information, and to
12 institute reasonable policies, procedures, and training programs to
13 educate its employees about protecting the confidentiality of
14 patients' personal health information. Plaintiff further alleges that
15 Defendants *solicited and received consideration from Plaintiff for*
16 *this implicit promise, including monies paid for medical services*
17 *and confidential medical information*, and that Defendants
18 breached the parties implied in fact agreement by transmitting
19 personally identifiable, health information to Facebook and Google
20 via tracking tools on its website and failing to develop policies,
21 procedures, processes, and notices to ensure that would not
22 happen.

23 No. C22-7646, 2023 WL 4996117, at *3 (Mo. Cir. Ct. July 20, 2023) (internal citations omitted)
24 (emphasis added). Similarly, in *Doe v. Regents*, the court held that plaintiff had plausibly alleged
the parties had entered into an implied contract where:

Plaintiff alleges that she and other class members *paid money and*
provided their User Data to UC Regents in exchange for services,
and that she and class members would not have entrusted UC
Regents with their User Data in the absence of an implied contract
obligating UC Regents to safeguard that data. She states that UC
Regents breached this implied contract by disclosing that
information to Meta, a third party. She contends that she would not
have paid, or would have paid less, for these services had she
known that UCSF would disclose her data.

672 F. Supp. 3d at 821 (emphasis added); *see also C.M. v. MarinHealth Medical Group, Inc.*, No. C23-4179, 2024 WL 217841, at *4 (N.D. Cal. Jan. 19, 2024) (“In contrast, this case arises in the context of *paid* healthcare services and is based on an ongoing relationship between the parties that plaintiff alleges was based in part, or that the amount he paid for the services was based in part, on MarinHealth’s security promises. In this context, adequate consideration has been alleged for the implied contract claim.” (emphasis in original)). In contrast, Plaintiff here alleges that the provision of user data *alone* to Defendant in exchange for services was sufficient to establish an implied in fact contract. Dkt. No. 1 ¶¶ 189–91. Plaintiff did not even argue that she paid for services in her brief in response to this argument. *See* Dkt. No. 21 at 18–19. And while “[m]any federal courts have held that an implied contract to safeguard customers’ sensitive data could reasonably be found to exist in transactions where consumers are solicited or invited to provide personal information in exchange for a good or service,” Plaintiff alleges no invitation or solicitation by Defendant indicating that it implicitly assented to secure PHI and PII in exchange for remuneration. *See In re Mednax Services, Inc., Customer Data Security Breach Litigation*, 603 F. Supp. 3d 1183, 1221 (S.D. Fla. 2022). “Plaintiff[’s] allegations reveal only that [she] provided [her] personal information as required to receive healthcare services from Defendant[]—not data security services beyond the privacy requirements already imposed on Defendant[] by federal law.” *Id.*; *see also* Dkt. No. 1 ¶¶ 188–94.

Plaintiff also argues that Defendant’s Notice of Privacy Practices can form the basis of an implied contract. Dkt. No. 21 at 19. However, as the court in *Doe v. Regents* noted, while such policies may form the *terms* of an implied contract, they do not alone serve as an enforceable contract without a separate “meeting of the minds” between the parties. *See* 672 F. Supp. 3d at 821. Because privacy notices serve to inform patients of their rights under federal law and the duties imposed on healthcare providers by these statutory provisions, they are not contractual in

1 nature. *See In re Mednax*, 603 F. Supp. 3d at 1222 (citing *Brush v. Miami Beach Healthcare*
2 *Grp. Ltd.*, 238 F. Supp. 3d 1359 (S.D. Fla. 2017)). “Because Defendant[is] required by law to
3 adhere to HIPAA without receiving any consideration from Plaintiff[] or any other patient, these
4 provisions cannot create contractual obligations.” *Id.*; *see also Griffey v. Magellan Health*
5 *Incorporated*, 562 F. Supp. 3d 34, 52 (D. Az. 2021) (“Plaintiffs here fail to allege consideration
6 because they did not allege that Magellan promised to act beyond the existing HIPPA
7 mandates.”). Accordingly, the Court cannot infer from Plaintiff’s allegations the mutual assent
8 and meeting of the minds required to form an implicit contract for data security services based on
9 the Parties’ conduct.

10 Finally, with respect to damages, Defendant argues that the damages Plaintiff seeks—the
11 lost property value of her personal information (Dkt. No. 21 at 24)—are not recoverable in
12 contract (Dkt. No. 17 at 19). While the Ninth Circuit has not directly addressed this issue, courts
13 in this circuit have dismissed cases where, like here, plaintiff’s injury is based on “‘the loss of
14 the inherent value of their personal data,’ as well as where it was undisputed that plaintiffs paid
15 no money to the defendant.” *Eisenhower Med. Ctr.*, 2024 WL 878100, at *6 (quoting *Doe v.*
16 *Meta Platforms, Inc.*, No. C22-3580, 2023 WL 5837443, at *15 (N.D. Cal. Sept. 7, 2023)); *see*
17 *also Saeedy v. Microsoft Corp.*, No. C23-1104, 2021 WL 8828852, at *6 (W.D. Wash. Dec. 21,
18 2023) (“To establish standing for their claims of loss of value in their data as property, Plaintiffs
19 must show that they personally lost money or property as a result of Microsoft’s conduct.”).
20 Because, as discussed above, Plaintiff has made no allegations that she ever paid Defendant, she
21 has not alleged damages for her breach of contract claim.

22 For the foregoing reasons, Plaintiff’s breach of implied contract claim is DISMISSED with
23 leave to amend.

F. Count V: Unjust Enrichment

Plaintiff brings a claim for unjust enrichment on behalf of herself and the putative national class. Dkt. No. 1 ¶¶ 195–200. Defendant contends that Plaintiff has failed to plead sufficient facts showing that Defendant received a benefit, that Plaintiff suffered a detriment, and that it would be unjust for Defendant to retain any benefit without payment. Dkt. No. 17 at 20.

Unjust enrichment “occurs when one retains money or benefits which in justice and equity belong to another.” *Bailie Commc’ns, Ltd. v. Trend Bus. Sys., Inc.*, 61 Wn. App. 151, 160, 810 P.2d 12 (1991). This cause of action “is the method of recovery for the value of the benefit retained absent any contractual relationship because notions of fairness and justice require it.” *Young*, 164 Wn.2d at 484 (citing *Bailie Commc’ns*, 61 Wn. App. at 160). To state a claim for unjust enrichment, Plaintiff must show that: (1) Plaintiff conferred a benefit upon Defendant, (2) at Plaintiff’s expense, and (3) the circumstances make it unjust for Defendant to retain the benefit without payment. *Young*, 164 Wn.2d at 484.

“A person confers a benefit upon another if he gives to the other possession of or some other interest in money, land, chattels, or choses in action, performs services beneficial to or at the request of the other, satisfies a debt or a duty of the other, or in any way adds to the other's security or advantage.” *Chandler v. Washington Toll Bridge Authority*, 17 Wn.2d 591, 601, 137 P.2d 97 (1943). Even though the Court has already determined that Plaintiff has not made sufficient factual allegations as to what information she specifically provided to Defendant, the provision of any PHI to Defendant would be sufficient to confer a benefit. *See Boone Health*, 2023 WL 4996117, at *4 (finding that plaintiff had conferred a benefit on defendants in the form of valuable and confidential medical information); *see also In re Capital One Consumer Data Security Breach Litig.*, 488 F. Supp. 3d 374, 412–13 (E.D. Va. 2020) (finding that benefit was conferred to Amazon where it “profited from its storage and retention of Plaintiffs’ PII”).

1 That said, Plaintiff fails to adequately plead either a concrete detriment or that the
2 circumstances in this case make it unjust for Defendant to retain any benefit conferred. Plaintiff
3 generically contends that she “suffered from: ‘(i) invasion of privacy, (ii) lost time and
4 opportunity costs associated with attempting to mitigate the actual consequences of the Pixel,
5 (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information,
6 (v) statutory damages, and (vi) the continued and ongoing risk to their Private Information.’”
7 Dkt. No. 21 at 21 (quoting Dkt. No. 1 ¶ 33). But she fails to provide any factual support for these
8 vague assertions set forth in a section entitled “Purpose of this Lawsuit.” *See generally* Dkt. No.
9 1 ¶¶ 20–34, 35–42. For example, Plaintiff does not specifically contend that she spent any time
10 undertaking data security measures, resetting account passwords, or monitoring bank statements
11 for unauthorized account use in support of her assertion that she “lost time and opportunity costs
12 associated with attempting to mitigate the actual consequences of the Pixel” (Dkt. No. 21 at 21;
13 Dkt. No. 1 ¶ 33). Nor does Plaintiff make contentions regarding the specific private information
14 she contends that she shared with Defendant and that Defendant, in turn, shared to third parties.
15 Without this factual support—all of which is within Plaintiff’s personal knowledge—Plaintiff
16 has not plead a concrete detriment for purposes of an unjust enrichment claim.

17 Finally, the Court addresses Plaintiff’s argument that she has adequately shown that it
18 would be unjust for Defendant to retain the benefit conferred. First, Plaintiff has not made
19 allegations that Defendant has received financial compensation from Plaintiff as a result of
20 providing medical services.⁶ None of the citations to the Complaint that Plaintiff points to
21 include the allegation that Plaintiff ever paid Defendant for the provision of medical services.

22
23 ⁶ Plaintiff claims that “similar” claims were upheld in *Doe v. Meta Platforms*. Dkt. No. 21 at 21–22. That case is
24 inapt as it discusses an unjust enrichment claim in the context of Defendant Meta Platforms, Inc. selling plaintiffs’
data and unjustly retaining the proceeds which is not the situation alleged in this case. *See Meta Platforms*, 2023 WL
5837443, at *13.

1 See Dkt. No. 1 ¶¶ 38, 191, 193; Dkt. No. 21 at 26. Plaintiff must plead all relevant facts in the
2 complaint itself, rather than relying on facts pleaded in briefs, to meet the pleading requirements.
3 See *Finley v. TransUnion*, No. C17-7165, 2019 WL 3238903, at *3 (N.D. Cal. July 18, 2019).
4 Plaintiff also argues that Defendant has “benefitted from the disclosure of Plaintiffs’ Private
5 Information for marketing and retargeting.” Dkt. No. 21 at 21. Plaintiff makes minimal
6 allegations as to Defendant’s use of the Pixel and subsequent retargeting campaigns. However,
7 taking the pleadings in the light most favorable to Plaintiff—and bearing in mind that the
8 specifics of Defendant’s marketing costs are not visible to Plaintiff at this stage in litigation—
9 Plaintiff’s allegation that “[b]y utilizing the Pixel, the cost of advertising and retargeting was
10 reduced, thereby benefitting Defendant” would be sufficient to plead a retention of monetary
11 benefits by Defendant for purposes of Plaintiff’s unjust enrichment claim and for the narrow
12 purpose of surviving a motion to dismiss. See Dkt. No. 1 ¶ 135; *Boone Health*, 2023 WL
13 4996773, at *4 (finding that defendants’ monetizing of advertising benefits sufficient to state a
14 claim for unjust enrichment on a motion to dismiss).

15 For the foregoing reasons, Plaintiff’s unjust enrichment claim is DISMISSED with leave to
16 amend.

17 **G. Counts VI–VIII: Violations of the Electronic Communications Privacy Act**
18 **(“ECPA”), 18 U.S.C. § 2510, et seq.**

19 Plaintiff brings three claims under the ECPA on behalf of herself and the putative
20 national class: unauthorized interception, use, and disclosure pursuant to 18 U.S.C. § 2511(1)
21 (Count VI); unauthorized divulgence by electronic communications service pursuant to 18
22 U.S.C. § 2511(3)(a) (Count VII); and unauthorized disclosure of communications while in
23 electronic storage by an electronic communications service pursuant to 18 U.S.C. § 2702(a)(1)
24 (Count VIII). Dkt. No. 1 ¶¶ 201–58. Defendant contends that each of these claims fails because

1 Plaintiff has failed to allege any unlawful interception, there is no civil liability for procuring an
2 interception by a third party, Plaintiff has failed to show that the contents of any communications
3 were disclosed to a third party, and Defendant is not a provider of an electronic communications
4 service under either Section 2511(3)(a) or 2702(a)(1) of the ECPA. Dkt. No. 17 at 20–27.

5 All three of Plaintiff’s claims under the ECPA (18 U.S.C. § 2510, *et seq.*) “require[] a
6 showing that the defendant ‘(1) intentionally (2) intercepted, endeavored to intercept or procured
7 another person to intercept or endeavor to intercept (3) the contents of (4) an electronic
8 communication, (5) using a device.’” *See In re Facebook Internet Tracking Litig.*, 263 F. Supp.
9 3d 836, 844 (N.D. Cal. 2017) (quoting *In re Google Cookie Placement Consumer Privacy Litig.*,
10 806 F.3d 125, 135 (3d Cir. 2015)).

11 Defendant first argues that “Plaintiff cannot establish that any communication has been
12 unlawfully ‘intercepted’ by Overlake,” because the ECPA is a one-party consent statute. Dkt.
13 No. 17 at 21 (citing 18 U.S.C. § 2511(2)(d)). Under the ECPA, it is not unlawful for a person to
14 intercept electronic communications “where such person is a party to the communication,” as
15 Defendant is here. 18 U.S.C. § 2511(2)(d); *see also In re Facebook, Inc. Internet Tracking*
16 *Litigation*, 956 F.3d 589, 607 (9th Cir. 2020) (“Both [the ECPA and CIPA] contain an exemption
17 from liability for a person who is a ‘party’ to the communication, whether acting under the color
18 of law or not.”); *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 274 (3d Cir.
19 2016) (“Here, Google was either a party to all communications with the plaintiffs’ computers or
20 was permitted to communicate with the plaintiffs’ computers by Viacom, who was itself a party
21 to all such communications.”); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 519 (C.D. Cal. 2021)
22 (“Whereas in *In re Facebook* the plaintiffs alleged *Facebook* recorded communications between
23 the plaintiffs and third parties to which Facebook was *not* a party, here, Plaintiff alleges Nike and
24 FullStory recorded Plaintiff’s communications with Nike.”). It is clear from Plaintiff’s complaint

1 that Defendant was a party to Plaintiff’s website communications, and Plaintiff does not dispute
2 this contention. *See* Dkt. No. 1; Dkt. No. 21 at 22–23. To the extent that Plaintiff alleges that
3 Defendant surreptitiously recorded its own communications with Plaintiff, the Court finds that
4 the one-party consent exemption applies.

5 Because Defendant was a party to the at-issue communications, the issue becomes
6 “whether the alleged conduct was conducted with criminal and/or tortious intent under the
7 statute, such that it would qualify for the exception that renders the party exception
8 inapplicable.” *Eisenhower Med. Ctr.*, 2024 WL 878100, at *5. Courts within this Circuit have
9 held “that a plaintiff must plead sufficient facts to support an inference that the offender
10 intercepted the communication for the purpose of a tortious or criminal act that is *independent of*
11 the intentional act of recording or interception itself.” *Id.* (emphasis in original) (citing *Pena v.*
12 *GameStop*, 670 F. Supp. 3d 1112, 1119 (S.D. Cal. 2023)).

13 Plaintiff argues that Overlake’s “act of *recording* Plaintiff’s and Class Members’
14 communications” is distinct from the *transmission* of those communications to third parties, and
15 that such transmission is an independent tortious or criminal act. Dkt. No. 21 at 23. But “Plaintiff
16 points to no legal authority providing that the exception to § 2551(2)(d) is triggered when, as
17 here, the tortious conduct is the alleged wiretapping itself.” *Pena*, 670 F. Supp. 3d at 1119
18 (quoting *In re Google Cookie*, 806 F.3d at 145). *Pena* is instructive here: in *Pena*, plaintiffs
19 alleged that GameStop covertly created secret transcripts of all communications through the chat
20 feature on its website, which it then shared with Zendesk, a third party that harvests highly
21 personal data from chat transcripts for sales and marketing purposes. *Id.* at 1115. The alleged
22 conduct in *Pena* was significantly more bifurcated than the conduct alleged here, where Plaintiff
23 alleges the simultaneous transmission of communications to third parties like Facebook (*see* Dkt.
24 No. 1 ¶ 61), yet the court declined to distinguish between the act of *recording* and the act of

1 *transmitting. Pena*, 670 F. Supp. 3d at 1120. Further, the “criminal or tortious acts contemplated
 2 by § 2511(2)(d) are acts secondary to the acquisition of the communication involving tortious or
 3 criminal use of the interception’s fruits.” *Id.* (quoting *In re Google Cookie*, 806 F. Supp. 3d at
 4 145). Plaintiff fails to plead a tortious or criminal use of the acquired communications, separate
 5 from the recording, interception, or transmission. *See generally* Dkt. No. 1. For this reason, the
 6 tortious or criminal act exception does not apply here.⁷

7 For the foregoing reasons, Plaintiff’s ECPA claims are DISMISSED with leave to amend.

8 **H. Count IX: Violation of the Computer Fraud and Abuse Act (18 USC 1030, *et seq.*)**

9 Plaintiff brings a claim under the Computer Fraud and Abuse Act (“CFAA”) on behalf of
 10 herself and the putative national class. Dkt. No. 1 ¶¶ 259–66. Defendant argues that Plaintiff fails
 11 to plead that Defendant exceeded its authorized access or any direct costs as defined under the
 12 CFAA. Dkt. No. 17 at 27–28.

13 A defendant is liable under the CFAA when they “intentionally accesses a computer
 14 without authorization or exceed[] authorized access, and thereby obtain[] (A) information
 15 contained in a financial record of a financial institution, . . . (B) information from any department
 16 or agency of the United States, or (C) information from any protected computer.” 18 U.S.C.
 17 § 1030(a)(2). “‘Exceeds authorized access’ means to access a computer with authorization and to
 18 use such access to obtain or alter information in the computer that the accesser is not entitled so
 19 to obtain or alter.” 18 U.S.C. § 1030(e)(6).

20 Plaintiff argues that “[w]here a defendant accesses information from a protected
 21 computer under false pretenses – such as here, where a hidden tracking device was employed by
 22 Defendant to copy and transmit information from a protected computer – . . . the access is

23
 24 ⁷ Because the Court has determined that Plaintiff has not alleged the first prong of an ECPA claim, it declines to address the Parties’ additional arguments with respect to Plaintiff’s ECPA claims.

1 unauthorized.” Dkt. No. 21 at 28 (citing *America Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444
2 (E.D. Va. 1998)). Plaintiff relies on *America Online* for the proposition that because Defendant’s
3 access to Plaintiff’s communications was obtained under false pretenses, “Defendant’s entire
4 access to the information contained in Plaintiff’s communications and devices was illegitimate.”
5 Dkt. No. 21 at 28. *America Online* dealt with defendants who “harvested, or collected, the e-mail
6 addresses of AOL members in violation of AOL’s Terms of Service,” and who maintained AOL
7 accounts in order to harvest the email addresses of AOL members. 46 F. Supp. 2d at 448.
8 According to the court, the AOL defendants *viewed* the email addresses of other members with
9 authorization, but used such access to *harvest* those email addresses, which they were not
10 entitled to do. *Id.* at 450.

11 However, *America Online* preceded *Van Buren v. United States*, 593 U.S. 374 (2021),
12 which explicitly holds that access in violation of webpage terms of service does not “exceed
13 authorized access” for purposes of the CFAA. In *Van Buren*, a former police sergeant ran a
14 license-plate search in a law enforcement computer database in exchange for money. 593 U.S. at
15 378. The defendant in *Van Buren* “accessed the law enforcement database system with
16 authorization,” “even though he obtained information from the database for an improper
17 purpose.” *Id.* at 396. The Court held that Van Buren did not “exceed authorized access,” and
18 specifically opined about the application of the “exceeds authorized access” clause to violations
19 of computer use policies, saying:

20 As discussed, the Government reads the “exceeds authorized
21 access” clause to incorporate purpose-based limits contained in
22 contracts and workplace policies. . . . Many websites, services, and
23 databases—which provide “information” from “protected
24 computer[s],” § 1030(a)(2)(C)—authorize a user’s access only
 upon his agreement to follow specified terms of service. If the
 “exceeds authorized access” clause encompasses violations of
 circumstance-based access restrictions on employers’ computers, it
 is difficult to see why it would not also encompass violations of

1 such restrictions on website providers' computers. . . . In sum, an
2 individual "exceeds authorized access" when he accesses a
3 computer with authorization but then obtains information located
in particular areas of the computer—such as files, folders, or
databases—that are off limits to him.

4 *Id.* at 394–97. Although Plaintiff frames her argument as a question of whether Defendant's
5 authorization was legitimately obtained, she does not cite to any caselaw post-dating *Van Buren*
6 that supports such an interpretation of use restrictions invoked by a website's terms of use. For
7 this reason, the Court must find that Defendant did not exceed authorized access or otherwise
8 intentionally access a computer without authorization for purposes of a CFAA claim.

9 For the foregoing reasons, Plaintiff's CFAA claim is DISMISSED with leave to amend.

10 **I. Count X: Washington Consumer Protection Act ("CPA") (RCW 19.86.020)**

11 Plaintiff brings a claim under the CPA on behalf of herself and the putative national class.
12 Dkt. No. 1 ¶¶ 267–76. Defendant argues that Plaintiff has failed to establish injury to her
13 business or property. Dkt. No. 17 at 29.

14 The CPA provides that "[u]nfair methods of competition and unfair or deceptive acts or
15 practices in the conduct of any trade or commerce are hereby declared unlawful." RCW
16 19.86.020. "To prevail in a private CPA claim, the plaintiff must prove (1) an unfair or deceptive
17 act or practice, (2) occurring in trade or commerce, (3) affecting the public interest, (4) injury to
18 a person's business or property, and (5) causation." *Panag v. Farmers Ins. Co. of Wash.*, 166
19 Wn.2d 27, 37, 204 P.3d 885 (2009) (citing *Hangman Ridge Stables, Inc. v. Safeco Title Ins. Co.*,
20 105 Wn.2d 778, 784, 719 P.2d 531 (1986)). Either an unfair or a deceptive act can be the basis
21 for a CPA claim. *Klem v. Wash. Mut. Bank*, 176 Wn.2d 771, 787, 295 P.3d 1179 (2013).

22 The Parties dispute whether Plaintiff has sufficiently alleged an injury under the CPA.
23 And while the Court finds that Plaintiff has not adequately alleged an injury, the Court disagrees
24 that Plaintiff must allege it is a participant in the market for private information in order to show

1 injury. In *Guy v. Convergent Outsourcing, Inc.*, the court found that Plaintiffs had alleged injury
2 without allegations of participation in the market for private information. No. C22-1558, 2023
3 WL 4637318, at *8 (W.D. Wash. July 20, 2023) (“Plaintiffs assert that the diminished value of
4 their PII and the lost time spent remedying the PII disclosure are compensable. The allegations of
5 the lost value of the PII are sufficient to show an injury, because ‘the injury requirement is met
6 upon proof the plaintiff’s property interest or money is diminished because of the unlawful
7 conduct even if the expenses caused by the statutory violation are minimal.’” (quoting *Panag*,
8 204 P.3d at 899)). But in *Guy*, plaintiffs provided significantly more substantial allegations
9 regarding injury than Plaintiff has here:

10 To satisfy concerns about standing and injury, Plaintiffs provide
11 allegations about the value of their PII and the other injuries they
12 have suffered. First, Plaintiffs allege that as a result of the
13 Convergent data breach their PII has lost economic value because
14 it is now readily available, and they received nothing in return for
15 its disclosure. Plaintiffs allege on information and belief that their
16 PII is now available for sale on the “Dark Web,” and that it may
17 have a value ranging from \$40 to \$363, depending on the
18 sensitivity of the information. Plaintiffs also allege that there is an
19 “active and robust legitimate market,” which is referred to as the
“data brokering industry,” through which individuals can sell their
person data for up to \$50 a year. Plaintiff Guy believes his PII has
already been sold to criminals, given that he now receives many
spam phone calls and emails daily after the data breach, but not
before. Second, Plaintiffs allege that they have spent time trying to
monitor fraudulent activity arising from the data breach. This
includes Plaintiff Tanner who found \$100 fraudulent charge on
Netflix that he spent several hours disputing (though he does not
allege any out-of-pocket costs).

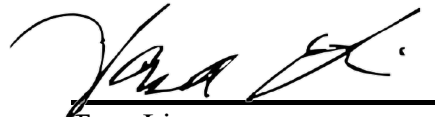
20 2023 WL 4637318, at *1 (internal citations omitted). Plaintiff here makes no such allegations
21 regarding her injury; without more specific allegations, her CPA claim cannot survive.

22 For the foregoing reasons, Plaintiff’s CPA claim is DISMISSED with leave to amend.
23
24

IV. CONCLUSION

Accordingly, the Complaint is DISMISSED in its entirety with leave to amend except for Plaintiff's Breach of Confidence claim which is dismissed with prejudice.

Dated this 13th day of May 2024.


Tana Lin
United States District Judge